Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

QUANTUM COMPUTING

[1]Mr. Naveen Kumar Kedia, [2]Akshat Singh, [3]Arpit Raychand Sansi, [4]Deven kumawat

[1] Assistant Professor, Department of Information Technology, JECRC College
[2]B.Tech Student, Department of Information Technology, JECRC College
[3]B.Tech Student, Department of Information Technology, JECRC College
[4]B.Tech Student, Department of Information Technology, JECRC College

ABSTRACT

This research paper considers the many possibilities of quantum computing, exploring both established and unexplored areas. From quantum algorithms to functional logic gates, this research explores the current state of quantum computing, highlighting progress and ongoing challenges. This main research interests include decoherence dynamics, complex quantum measurements, and the search for unified quantum descriptions.

The project addresses the complexity of decoherence, shows arguments that break symmetryand gives insight into irreversibility in a system by exploring entropy-like parameters.Although the success of relativity remains to be seen, the report highlights the importance ofunderstanding and controlling quantum measurements and recognizing quantum propertiesshared by inspections and inspectors. Report on the interaction between theoretical progressand practical application, showing the need to move from observation to control of quantum effects. As electronic circuits reach the quantum world, the discovery of quantum materialsrequires not only theoretical innovations but also practical applications of quantum concepts. Looking ahead, the paper shows successful development for quantum computing. The constant race to shrink the electric field is based on the nature of quantum reality, and the combination of theoretical development and technological development is the key to a new challenge. Although the future is still uncertain, the combination of theoretical insights and practical applications promises a quantum future full of problems and undeniable potential, pushing quantum computing to the brink of ground-breaking discoveries and advances.

Keywords: Cryptography, Quantum computing, Qubits, Quantum safe-cryptography, post-quantum cryptography.

[1] INTRODUCTION

1.1 Understanding Quantum Computing:

Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

Quantum computing marks a fundamental shift in information processing, leveraging the complexities of quantum mechanics. While traditional computers rely on bits, quantum computers utilize quantum bits, or qubits, capable of existing in a superposition of $|0\rangle$ and $|1\rangle$ simultaneously. Figure 1 illustrates the Bloch sphere, providing a visual representation of the vast spectrum of values a qubit can adopt. Unlike bits, which offer two discrete values, qubits enable the storage of information across a two-dimensional continuum, resembling the surface of a sphere.

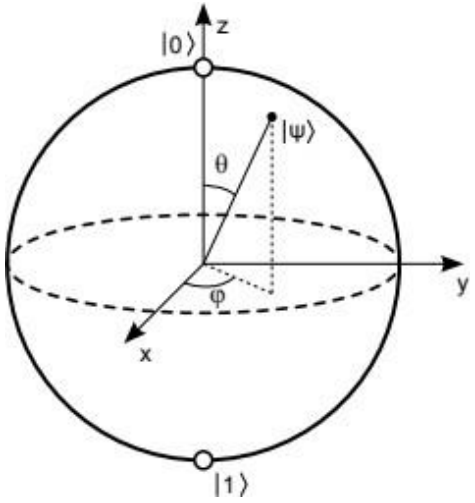

Fig 1 The Bloch Sphere

Quantum computing leverages the unique properties of qubits, allowing for operations not confined to predetermined values such as $|0\rangle$ or $|1\rangle$. Instead, quantum computers can simultaneously process all possible superpositions, providing a distinct efficiency advantage over classical binary computing in selected tasks. This capability opens the door to computational possibilities not currently accessible with classical computers, showcasing a speed advantage for specific problems.

[2] RELATED WORK

Implications for Data Protection:

The advent of quantum computing introduces profound implications for data protection, prompting a critical examination of its impact on data security and the confidentiality of communications. The potential risks are manifold, with one significant concern being the ability to compromise existing cryptographic systems, thereby posing severe threats to IT security. This risk extends to the very core of internet security protocols, impacting systems that rely on security, privacy, and trust.

Impact on Public-Key Cryptography:

Public-key cryptography, a cornerstone of secure communication, relies on cryptographic protocols like the Rivest-Sharmir-Adleman (RSA) algorithm. The security of this method hinges on the use of private and public keys for encryption. However, the advent of powerful quantum computers introduces a vulnerability, allowing adversaries to jeopardize public-key cryptography systems. Quantum computers with sufficient computational power could carry out decryption without prior knowledge of the private key, thereby compromising digital signatures, essential internet protocols like HTTPS (TLS), and security measures in online banking and shopping.

Impact on Symmetric Cryptography:

The obstacles presented by quantum computing also affect symmetric cryptography, demonstrated by commonly utilized standards like the Advanced Encryption Standard (AES).Symmetric and asymmetric cryptography are often employed together, as seen in the use of HTTPS. Symmetric cryptography necessitates secure key exchange methods for data confidentiality. However, existing key exchange methods may be susceptible to quantum computing risks, necessitating a comprehensive reassessment of data security measures to ensure the entire key exchange process remains secure.

Fig 2 IBM Quantum Computer

Retrospective Decryption:

The rapid advancement in binary computing hardware, characteristic of contemporary classical computers, poses a threat to IT security. With increasing computing power at decreasing costs, the retrospective decryption of historical data becomes a tangible concern, especially if the key lengths employed at the time were insufficiently long. Security experts regularly advocate for longer key lengths to ensure data security for a given period. Some governments' secret services

are reported to collect data deliberately for future retrospective decryption. Quantum computers, operating on different principles, introduce the potential for retrospective decryption much earlier in many cases.

[3] METHODOLOGY

Practical Quantum Computers:

The realization of practical quantum computers, capable of executing algorithms with tangible impacts, presents a formidable technological challenge. In 2019, Google claimed to have demonstrated quantum supremacy with a 54-qubit quantum computer, showcasing computational abilities that would take thousands of years for a powerful non-quantum supercomputer to perform. However, the practical significance of the demonstrated task was limited, serving more as a proof of concept. Despite potential advancements in this decade, building a large and usable quantum computer within the next ten years remains highly unlikely, though difficult to predict. The unpredictability surrounding the development of quantum computing introduces risks for current IT security, emphasizing the need for vigilance and preparation.

Post-Quantum Cryptography:

Addressing the security challenges posed by quantum computing involves the exploration of post-quantum cryptography or quantum-safe cryptography. This approach focuses on cryptographic systems whose security remains unaffected by the capabilities of quantum computers. Achieving quantum resilience involves the use of mathematical building blocks that quantum computers cannot solve more efficiently than classical computers.

While post-quantum cryptography offers a potential solution, its adoption is not without challenges. The transition to post-quantum cryptography is not standardized as of now, and it is anticipated to come with performance drawbacks. Larger computing resources are expected to be required for encryption, decryption, and signature operations, as well as additional networking resources for the exchange of longer keys and certificates. The development of post-quantum cryptography is an active area of research, with organizations like the US National Institute of Standards and Technology (NIST) working towards establishing a post-quantum cryptography standard.

As of 2020, prototypes of post-quantum cryptography, albeit non-standardized, are available for testing in various forms, including source code, software libraries (e.g., for OpenSSL), cloud services (e.g., Amazon AWS and Cloudflare), and consumer software (e.g., Google Chrome). The estimated timeline for a full transition to post-quantum cryptography could extend over 15-20 years in practice.

Organizations face the complex task of determining the duration for which they need to guarantee absolute confidentiality of data and protection from retrospective decryption. While an immediate threat from quantum computers may not be apparent in the foreseeable future, the uncertainty surrounding the timeline for building a usable quantum computer raises

concerns. For data that requires long-term security, this uncertainty poses a challenge, potentially necessitating an early transition to post-quantum cryptography.

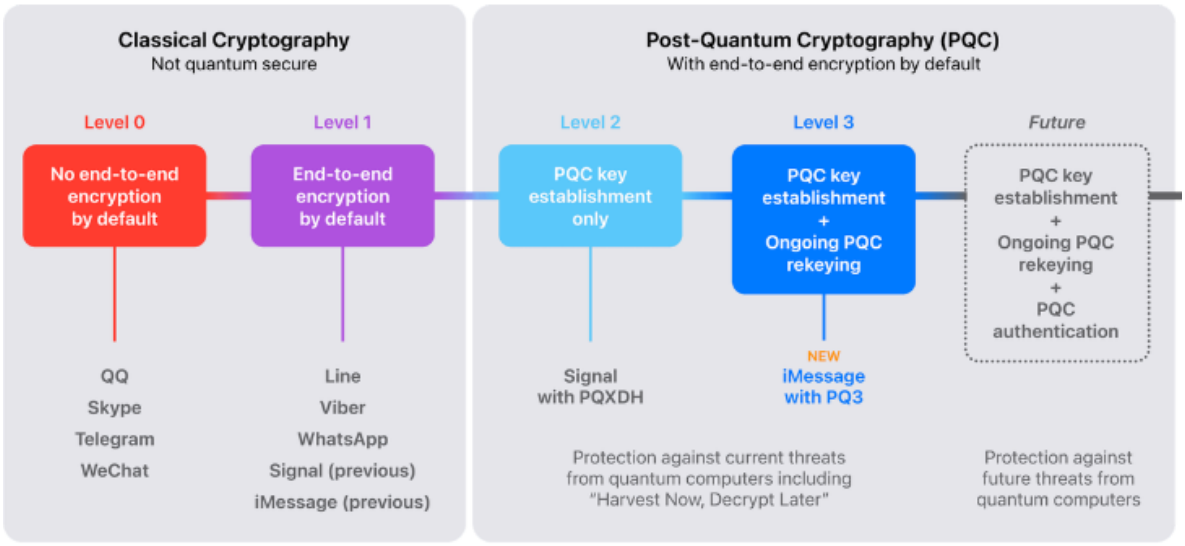

Fig 3 Quantum Cryptography

[4] CONCLUSION

The intersection of quantum computing and data protection introduces a multifaceted landscape of challenges and opportunities. While quantum computing holds the potential to revolutionize computation, it simultaneously poses threats to established cryptographic systems, requiring a proactive and strategic response from the information security community. The ongoing research and development in post-quantum cryptography underscore the importance of staying vigilant and adaptable in the face of evolving technologies. Organizations that prioritize comprehensive risk management, contingency planning, and adherence to evolving cryptographic standards will be better positioned to navigate the dynamic landscape of quantum computing and safeguard the confidentiality and integrity of sensitive information.

REFERENCES

[1] Machine Learning: Quantum vs Classical TARIQ M. KHAN, (Member, IEEE), ANDANTONIO ROBLES-KELLY, (Senior Member, IEEE-2020

[2] Quantum Vulnerability Analysis to Guide Robust Quantum Computing System Design FANG QI1 , KAITLIN N. SMITH2 , TRAVIS LECOMPTE3 , NIAN-FENG TZENG4 (Life Fellow, IEEE), XU YUAN5 (Senior Member, IEEE), FREDERIC T. CHONG6 (Fellow,

IEEE), AND LU PENG1 (Senior Member, IEEE)-2023

[3] Advances in Quantum Computation and Quantum Technologies: A Design Automation Perspective Giovanni De Micheli , Life Fellow, IEEE, Jie-Hong R. Jiang , Member, IEEE,

Robert Rand, Kaitlin Smith, Member, IEEE, and Mathias Soeken , Member, IEEE-2022

[4] G. Sentís, A. Monras, R. Muñoz-Tapia, J. Calsamiglia, and E. Bagan, ‘‘Unsupervised classification of quantum data,’’ Phys. Rev. X, vol. 9, no. 4, Nov. 2019, Art. no. 041029. [Online]. Available: https://link. aps.org/doi/10.1103/PhysRevX.9.041029

[5] P. Ronagh, ‘‘Quantum algorithms for solving dynamic programming problems,’’ 2019, arXiv:1906.02229. [Online]. Available: https://arxiv. org/abs/1906.02229

[6] A. Cornelissen, ‘‘Quantum gradient estimation and its application to quantum reinforcement learning,’’ M.S. thesis, Elect. Eng., Math. Comput. Sci., Delft Univ. Technol., Delft, The Netherlands, 2018.

[7] T. Fösel, P. Tighineanu, T. Weiss, and F. Marquardt, ‘‘Reinforcement learning with neural networks for quantum feedback,’’ Phys. Rev. X, vol. 8, no. 3, Sep. 2018, Art. no. 031084. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.8.031084

[8]J. Wallnfer, A. A. Melnikov, W. Dr, and H. J. Briegel, ‘‘Machine learning for long-distance quantum communication,’’ 2019, arXiv:1904.10797. [Online]. Available: https://arxiv.org/abs/1904.10797

[9] R. Iten, T. Metger, H. Wilming, L. del Rio, and R. Renner, ‘‘Discovering physical concepts with neural networks,’’ Phys. Rev. Lett., vol. 124, no. 1, Jan. 2020, Art. no. 010508. [Online].

Available: https://link.aps.org/ doi/10.1103/PhysRevLett.124.010508

[10] “IBM quantum systems,” Accessed: Jul. 28, 2022. [Online]. Available: https://quantum-computing.ibm.com/services?systems=all